CLAIMS

Sub B1

1. A method of proving entity membership in a nested group, wherein a presenter of credentials performs the step of presenting to a recipient of credentials one or more chains of group credentials.

2. The method of claim 1, wherein one of said chains of group credentials comprise one or more proofs of group membership.

3. The method of claim 2, wherein said proofs of group membership comprise one or more group membership certificates.

4. The method of claim 2, wherein said proofs of group membership comprise one or more group membership lists.

5. The method of claim 1, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

6. The method of claim 5, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

7. The method of claim 5, wherein said proofs of group non-membership comprise one or more group membership lists.

8. The method of claim 1, wherein said recipient is a resource server.

9. The method of claim 1, wherein said recipient is an on-line group server.

10. The method of claim 1, wherein said recipient is an on-line revocation server.

11. The method of claim 1, wherein said recipient is a client.

12. A method of proving entity non-membership in a nested group, wherein a presenter of credentials performs the step of presenting to a recipient of credentials one or more chains of group credentials.

13. The method of claim 12, wherein one of said chains of group credentials comprise one or more proofs of group membership.

14. The method of claim 13, wherein said proofs of group membership comprise one or more group membership certificates.

15. The method of claim 13, wherein said proofs of group membership comprise one or more group membership lists.

16. The method of claim 12, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

17. The method of claim 16, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

18. The method of claim 16, wherein said proofs of group non-membership comprise one or more group membership lists.

19. The method of claim 12, wherein said recipient is a resource server.

20. The method of claim 12, wherein said recipient is an on-line group server.

21. The method of claim 12, wherein said recipient is an on-line revocation server.

22. The method of claim 12, wherein said recipient is a client.

23. A computer system wherein a presenter of credentials presents to a recipient of credentials one or more chains of group credentials to prove entity membership in a nested group.

24. The system of claim 23, wherein one of said chains of group credentials comprise one or more proofs of group membership.

25. The system of claim 24, wherein said proofs of group membership comprise one or more group membership certificates.

26. The system of claim 24, wherein said proofs of group membership comprise one or more group membership lists.

27. The system of claim 23, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

28. The system of claim 27, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

29. The system of claim 27, wherein said proofs of group non-membership comprise one or more group membership lists.

30. The system of claim 23, wherein said recipient is a resource server.

31. The system of claim 23, wherein said recipient is an on-line group server.

32. The system of claim 23, wherein said recipient is an on-line revocation server.

33. The system of claim 23, wherein said recipient is a client.

34. A computer system wherein a presenter of credentials presents to a recipient of credentials one or more chains of group credentials to prove entity non-membership in a nested group.

35. The system of claim 34, wherein one of said chains of group credentials comprise one or more proofs of group membership.

36. The system of claim 35, wherein said proofs of group membership comprise one or more group membership certificates.

37. The system of claim 35, wherein said proofs of group membership comprise one or more group membership lists.

38. The system of claim 34, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

39. The system of claim 38, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

40. The system of claim 38, wherein said proofs of group non-membership comprise one or more group membership lists.

41. The system of claim 34, wherein said recipient is a resource server.

42. The system of claim 34, wherein said recipient is an on-line group server.

43. The system of claim 34, wherein said recipient is an on-line revocation server.

44. The system of claim 34, wherein said recipient is a client.

45. A method of operating a client device on a computer network, said client device requesting a service from a server and performing the steps of:

A. obtaining one or more chains of group credentials to prove client membership in a nested group, and

B presenting to the server a request for the service, said request including the chains of group credentials.

46. The method of claim 45, wherein one of said chains of group credentials comprise one or more proofs of group membership.

47. The method of claim 46, wherein said proofs of group membership comprise one or more group membership certificates.

48. The method of claim 46, wherein said proofs of group membership comprise one or more group membership lists.

49. The method of claim 45, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

50. The method of claim 49, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

51. The method of claim 49, wherein said proofs of group non-membership comprise one or more group membership lists.

52. A method of operating a client device on a computer network, said client device requesting a service from a server and performing the steps of:

A. obtaining one or more chains of group credentials to prove client non-membership in a nested group, and

B. presenting to the server a request for the service, said request including the chains of group credentials.

53. The method of claim 52, wherein one of said chains of group credentials comprise one or more proofs of group membership.

54. The method of claim 53, wherein said proofs of group membership comprise one or more group membership certificates.

55. The method of claim 53, wherein said proofs of group membership comprise one or more group membership lists.

56. The method of claim 52, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

57. The method of claim 56, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

58. The method of claim 56, wherein said proofs of group non-membership comprise one or more group membership lists.

59. A client device on a computer network requesting a service from a server, said client device comprising:

A. means for obtaining one or more chains of group credentials to prove client membership in a nested group, and

B. means for presenting to the server a request for the service, said request including the chains of group credentials.

60. The client device of claim 59, wherein one of said chains of group credentials comprise one or more proofs of group membership.

61. The client device of claim 60, wherein said proofs of group membership comprise one or more group membership certificates.

62. The client device of claim 60, wherein said proofs of group membership comprise one or more group membership lists.

63. The client device of claim 59, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

64. The client device of claim 63, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

65. The client device of claim 63, wherein said proofs of group non-membership comprise one or more group membership lists.

66. A client device on a computer network requesting a service from a server, said client device comprising:

A. means for obtaining one or more chains of group credentials to prove client non-membership in a nested group, and

B. means for presenting to the server a request for the service, said request including the chains of group credentials.

67. The client device of claim 66, wherein one of said chains of group credentials comprise one or more proofs of group membership.

68. The client device of claim 67, wherein said proofs of group membership comprise one or more group membership certificates.

69. The client device of claim 67, wherein said proofs of group membership comprise one or more group membership lists.

70. The client device of claim 66, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

71. The client device of claim 70, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

72. The client device of claim 70, wherein said proofs of group non-membership comprise one or more group membership lists.

73. A method for operating a resource server on a computer network, said resource server controlling access to one or more resources by a plurality of client devices and performing the steps of:

A. accepting resource access requests from the client devices, each request comprising one or more chains of group credentials proving client membership in a nested group,

B. validating the chains of group credentials, and

C. if the chains of group credentials are valid, authorizing the requested access.

74. The method of claim 73, wherein one of said chains of group credentials comprise one or more proofs of group membership.

75. The method of claim 74, wherein said proofs of group membership comprise one or more group membership certificates.

76. The method of claim 74, wherein said proofs of group membership comprise one or more group membership lists.

77. The method of claim 73, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

78. The method of claim 77, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

79. The method of claim 77, wherein said proofs of group non-membership comprise one or more group membership lists.

80. A method of operating a resource server on a computer network, said resource server controlling access to one or more resources by a plurality of client devices and performing the steps of:

A. accepting resource access requests from the client devices, each request comprising one or more chains of group credentials proving client non-membership in a nested group,

B. validating the chains of group credentials, and

C. if the chains of group credentials are valid, authorizing the requested access.

81. The method of claim 80, wherein one of said chains of group credentials comprise one or more proofs of group membership.

82. The method of claim 81, wherein said proofs of group membership comprise one or more group membership certificates.

83. The method of claim 81, wherein said proofs of group membership comprise one or more group membership lists.

84. The method of claim 80, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

85. The method of claim 84, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

86. The method of claim 84, wherein said proofs of group non-membership comprise one or more group membership lists.

87. A resource server on a computer network controlling access to one or more resources by a plurality of client devices, said resource server comprising:

A. means for accepting resource access requests from the client devices, each request comprising one or more chains of group credentials proving client membership in a nested group,

B. means for validating the chains of group credentials, and

C. if the chains of group credentials are valid, means for authorizing the requested access.

88. The resource server of claim 87, wherein one of said chains of group credentials comprise one or more proofs of group membership.

89. The resource server of claim 88, wherein said proofs of group membership comprise one or more group membership certificates.

90. The resource server of claim 88, wherein said proofs of group membership comprise one or more group membership lists.

91. The resource server of claim 87, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

92. The resource server of claim 91, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

93. The resource server of claim 91, wherein said proofs of group non-membership comprise one or more group membership lists.

94. A resource server on a computer network controlling access to one or more resources by a plurality of client devices, said resource server comprising:

A. means for accepting resource access requests from the client devices, each request comprising one or more chains of group credentials proving client non-membership in a nested group,

B. means for validating the chains of group credentials, and

C. if the chains of group credentials are valid, means for authorizing the requested access.

95. The resource server of claim 94, wherein one of said chains of group credentials comprise one or more proofs of group membership.

96. The resource server of claim 95, wherein said proofs of group membership comprise one or more group membership certificates.

97. The resource server of claim 95, wherein said proofs of group membership comprise one or more group membership lists.

98. The resource server of claim 94, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

99. The resource server of claim 98, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

100. The resource server of claim 98, wherein said proofs of group non-membership comprise one or more group membership lists.

101. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device requesting a service from a server, configures the network device to operate as a client device that:

A. obtains one or more chains of group credentials to prove client membership in a nested group, and

B. presents to the server a request for the service, said request including the chains of group credentials.

102. The computer data signal of claim 101, wherein one of said chains of group credentials comprise one or more proofs of group membership.

103. The computer data signal of claim 102, wherein said proofs of group membership comprise one or more group membership certificates.

104. The computer data signal of claim 102, wherein said proofs of group membership comprise one or more group membership lists.

105. The computer data signal of claim 101, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

106. The computer data signal of claim 105, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

107. The computer data signal of claim 105, wherein said proofs of group non-membership comprise one or more group membership lists.

108. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device requesting a service from a server, configures the network device to operate as a client device that:

A. obtains one or more chains of group credentials to prove client non-membership in a nested group, and

B. presents to the server a request for the service, said request including the chains of group credentials.

109. The computer data signal of claim 108, wherein one of said chains of group credentials comprise one or more proofs of group membership.

110. The computer data signal of claim 109, wherein said proofs of group membership comprise one or more group membership certificates.

111. The computer data signal of claim 109, wherein said proofs of group membership comprise one or more group membership lists.

112. The computer data signal of claim 108, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

113. The computer data signal of claim 112, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

114. The computer data signal of claim 112, wherein said proofs of group non-membership comprise one or more group membership lists.

115. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device controlling access to one or more resources by a plurality of client devices, configures the network device to operate as a resource server that:

A. accepts resource access requests from the client devices, each request comprising one or more chains of group credentials proving client membership in a nested group,

B. validates the chains of group credentials, and

C. if the chains of group credentials are valid, authorizes the requested access.

116. The computer data signal of claim 115, wherein one of said chains of group credentials comprise one or more proofs of group membership.

117. The computer data signal of claim 116, wherein said proofs of group membership comprise one or more group membership certificates.

118. The computer data signal of claim 116, wherein said proofs of group membership comprise one or more group membership lists.

119. The computer data signal of claim 115, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

120. The computer data signal of claim 119, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

121. The computer data signal of claim 119, wherein said proofs of group non-membership comprise one or more group membership lists.

122. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device controlling access to one or more resources by a plurality of client devices, configures the network device to operate as a resource server that:

A. accepts resource access requests from the client devices, each request comprising one or more chains of group credentials proving client non-membership in a nested group,

B. validates the chains of group credentials, and

C. if the chains of group credentials are valid, authorizes the requested access.

123. The computer data signal of claim 122, wherein one of said chains of group credentials comprise one or more proofs of group membership.

124. The computer data signal of claim 123, wherein said proofs of group membership comprise one or more group membership certificates.

125. The computer data signal of claim 123, wherein said proofs of group membership comprise one or more group membership lists.

126. The computer data signal of claim 122, wherein one of said chains of group credentials comprise one or more proofs of group non-membership.

127. The computer data signal of claim 126, wherein said proofs of group non-membership comprise one or more group non-membership certificates.

128. The computer data signal of claim 126, wherein said proofs of group non-membership comprise one or more group membership lists.